

**UNITED STATES DISTRICT COURT
DISTRICT OF MAINE**

IN THE MATTER OF THE SEARCH OF)
AN APPLE IPHONE SEIZED ON) Case No. 2:24-mj-206-KFW
AUGUST 16, 2023)

**AFFIDAVIT IN SUPPORT OF AN APPLICATION
FOR A WARRANT TO SEARCH AND SEIZE**

I, Thomas Lapierre, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a “federal law enforcement officer” within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant. I have been a Task Force Officer (“TFO”) with the U.S. Drug Enforcement Administration (“DEA”) since 2007 and I am presently assigned to the Portland, Maine, office. I have been a police officer since 2002.

2. As a law enforcement officer, I have received specialized training involving the use, possession, packaging, manufacturing, sales, concealment, and transportation of various controlled substances, money laundering techniques, and conspiracy investigations. I am also familiar with federal firearms laws.

3. During my assignment at the DEA, I have participated in narcotics investigations both as a case agent and in a supportive role. I have participated in the arrests of multiple drug traffickers and in interviewing informants and suspects concerning the methods and means of drug traffickers. I have also participated in countless static and mobile surveillance activities and assisted in the execution of

multiple search warrants and arrest warrants. I have conducted investigations regarding these unlawful activities, including violations of Sections 841(a)(1), 843(b), 846, 952(a), and 963 of Title 21 of the United States Code. I am aware based on my training and experience that drug traffickers often possess firearms to protect themselves, their narcotics, and proceeds from narcotics trafficking.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of 21 U.S.C. §§ 841, 843, and 846 (drug trafficking, unlawful use of a communications facility, and conspiracy to commit drug trafficking), 18 U.S.C. §§ 922(g)(1) (unlawful possession of a firearm by a prohibited person) and 1959 (violent crimes in aid of racketeering) have been committed by Nathaniel Ashwood.

LOCATION TO BE SEARCHED

5. The property to be searched is a black Apple iPhone with a cracked screen protector (hereinafter, the “Target Device”). The Target Device was seized in Rockingham, Vermont, on about August 16, 2023. Photos of the Target Device are shown below. The Target Device is currently located at the offices of the United States Drug Enforcement Administration in South Portland, Maine.



6. The applied-for warrant would authorize the forensic examination of the Target Device for the purpose of identifying electronically stored data particularly described in Attachment B.

ITEMS TO BE SEIZED

7. The items to be seized are set forth in Attachment B to the search warrant application.

SHOWING OF PROBABLE CAUSE

8. I adopt and incorporate my affidavit and attachments filed on November 22, 2023, in support of a search warrant for the Target Device (attached as Exhibit A).

9. Law enforcement executed the November 22, 2023, warrant for the Target Device and obtained a limited extraction of data from the phone. At the time of this

data extraction, law enforcement did not know the password to the Target Device. This warrant was returned to the Court on January 8, 2024.

10. Since this search, law enforcement has continued to make effort to access the password to the Target Device, which would allow for a more complete review of the contents. These efforts involve the use of forensic tools that attempt to guess the password over time.

11. The password was identified through use of forensic tools on June 9, 2024.

12. I have custody of the Target Phone and seek a new search warrant to perform another extraction of the contents. Based on my training and experience, I believe this extraction and search will yield additional data that was not previously accessible without the password.¹

TECHNICAL TERMS

13. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone

¹ On June 18, 2024, I connected the Target Device to forensic equipment and performed an extraction. I reviewed the extraction to ensure it was successful. I subsequently realized that the Court issued a warrant authorizing a phone examination in a separate investigation and had yet to issue a warrant for the Target Device. I deleted the extraction performed on the Target Device and will conduct a new extraction if this warrant issues.

number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use

removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.
- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes)

and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.

- f. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

14. Based on my training, experience, and research, I know that the Target Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

15. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

16. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Target Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Target Device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

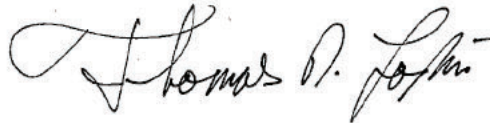
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

17. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

18. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

19. Based on the facts set forth above and in the attachments, there is probable cause to believe that violations of Title 21, United States Code, Sections 841(a)(1) (possession with intent to distribute controlled substances), 843 (unlawful use of a communications facility), and 846 (conspiracy), and Title 18, United States Code, Sections 922(g)(1) (possession of a firearm by a convicted felon) and 1959 (violent crimes in aid of racketeering), have been committed by Nathaniel Ashwood and that evidence of those criminal violations is likely to be found on the Target Device. I respectfully request that a search warrant be issued authorizing the examination of the Target Device to seek the items described in Attachment B.





Thomas Lapierre
Task Force Officer, DEA

Sworn to telephonically and signed
electronically in accordance with the
requirements of Rule 4.1 of the Federal Rules
of Criminal Procedures

Date: Jun 21 2024

City and state: Portland, Maine





Judge's signature

Karen Frink Wolf, U.S. Magistrate Judge
Printed name and title